
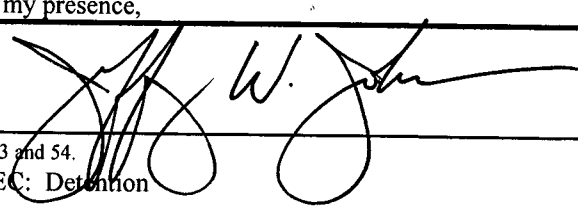


ORIGINAL

CRIMINAL COMPLAINT

UNITED STATES DISTRICT COURT		CENTRAL DISTRICT OF CALIFORNIA	
UNITED STATES OF AMERICA v. STANLEY ALEXANDER HUDSON.		DOCKET NO.	
		MAGISTRATE'S CASE NO. <b>08-08-2660M</b>	
Complaint for violation of Title 18, United States Code, Section 1029(a)(5)			
NAME OF MAGISTRATE JUDGE HONORABLE JEFFREY W. JOHNSON		UNITED STATES MAGISTRATE JUDGE	LOCATION Los Angeles, CA
DATE OF OFFENSE Date unknown through October 28, 2008	PLACE OF OFFENSE Los Angeles County, California	ADDRESS OF ACCUSED (IF KNOWN) <div style="border: 1px solid black; padding: 5px; display: inline-block;">FILED CLERK, U.S. DISTRICT COURT OCT 28 2008</div>	
<p>COMPLAINANT'S STATEMENT OF FACTS CONSTITUTING THE OFFENSE OR VIOLATION:</p> <p>Beginning on or about an unknown date, and continuing through October 28, 2008, in Los Angeles County, within the Central District of California, defendant STANLEY ALEXANDER HUDSON knowingly and with intent to defraud effected transactions, with one or more access devices issued to another person or persons, to receive payment or any other thing of value during a one-year period the aggregate value of which is equal to or greater than \$1,000.</p>			
BASIS OF COMPLAINANT'S CHARGE AGAINST THE ACCUSED: (See supporting affidavit)			
MATERIAL WITNESSES IN RELATION TO THIS CHARGE:			
Being duly sworn, I declare that the foregoing is true and correct to the best of my knowledge.		SIGNATURE OF COMPLAINANT ERIC SHEN 	
		OFFICIAL TITLE UNITED STATES POSTAL INSPECTOR, UNITED STATES POSTAL INSPECTION SERVICE	
Sworn to before me and subscribed in my presence,			
SIGNATURE OF MAGISTRATE JUDGE(1) 		DATE October 28, 2008	

1) See Federal Rules of Criminal Procedure rules 3 and 54.

AUSA: Harvinder S. Anand

REC: Detention

HSA

A F F I D A V I T

I, Eric Shen, being duly sworn, hereby depose and say:

I.

INTRODUCTION, TRAINING AND EXPERIENCE

1. I am a United States Postal Inspector with the United States Postal Inspection Service ("USPIS"), Los Angeles Division, and have been so employed since July 2005. As a U.S. Postal Inspector, my duties are to investigate violations of postal law, including credit card fraud, mail theft, mail fraud, and related financial crimes.

2. I have completed a twelve-week basic training course in Potomac, Maryland, which included training in Internet and mail fraud, and financial crime investigations. I am a member of the International Association of Financial Crimes Investigators ("IAFCI"). I attend IAFCI meetings, where a number of topics are discussed, including, but not limited to, identity fraud-related investigations. I am a member of the Los Angeles Identity Theft/Economic Crimes ("ITEC") Task Force.

3. I have conducted and participated in numerous investigations involving credit card fraud, mail theft, mail fraud, and other financial crimes, and have made numerous arrests of individuals committing such offenses. I have participated in the execution of search warrants which have resulted in the seizure of evidence related to these offenses. I have debriefed and used

informants who have provided information and assistance resulting in the federal prosecution of individuals committing financial crimes. Based on my training and experience, I am familiar with the *modus operandi* of persons involved in committing credit card fraud, mail theft, mail fraud, and other financial crimes.

4. Based upon my training and experience, and information related to me by other experienced law enforcement personnel who specialize in the investigation of financial and identity theft crimes, including access device fraud, wire fraud, and credit card fraud, I know the following:

a. Individuals involved in financial and identity theft schemes keep evidence of their schemes in their residences, automobiles, garages, and storage structures, such as account statements, applications, receipts, identity documents and convenience checks, and credit cards and driver's licenses related to those schemes.

b. Individuals in such schemes also frequently keep or maintain lists containing victim information, such as names, dates of birth, social security numbers, addresses, and other victim personal identification information.

c. Individuals involved in financial and identity theft schemes sometimes keep large amounts of cash at their residences. In one case in which I was involved, the search of a residence of

an individual involved in similar schemes resulted in the recovery of more than \$30,000.

d. Individuals involved in financial and identity theft schemes commonly use and maintain computers at their residence and business. Individuals who commit such crimes commonly use computers to track their fraudulent transactions. Suspects also often use computers to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the Internet. Suspects often use computers to:

- i. Apply on-line for fraudulent credit cards;
- ii. Obtain personal identification information for the purpose of establishing or modifying fraudulent credit card accounts;
- iii. Use fraudulently obtained credit cards to make purchases, including, sometimes, to purchase personal information of victims to commit identity theft; and
- iv. Keep records of their crimes.

5. Based upon my training and experience and information related to me by experienced agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during the search of the

premises it is not always possible to search digital devices for data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, software application or operating system that is being searched.

b. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Digital devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Because digital data are particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the digital devices from which the data will be extracted.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search

for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 240 million pages of data, that, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 GB drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital

device user can conceal text in an image file that cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that are concealed or encrypted to determine whether they are evidence, contraband or instrumentalities of a crime.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other experienced law enforcement officers and agents. In preparing this affidavit, I have consulted with other law enforcement officers and agents with many years of combined experience in the field of financial crime investigations. This affidavit is intended to show that there is sufficient probable cause for the requested complaint, arrest warrant, and search warrants, and does not purport to set forth all of my knowledge of or investigation into this matter.

## II.

### PURPOSE OF AFFIDAVIT

7. This affidavit is made in support of a criminal complaint against, and arrest warrant for, STANLEY ALEXANDER HUDSON ("HUDSON"), also known as Stanley Alexander, S. Alexander, S. A. Hudson, S. A. Alexander, S. S. Alexander, Stanley A. Hudson and Josh V. Webber, for violation of Title 18, United States Code, Section 1029(a)(5) (Access Device Fraud).

8. This affidavit is also made in support of an application for authorization to search the residence located at 205 West Fairview Boulevard, Inglewood, California 90302 ("SUBJECT PREMISES-1") and a dark grey color BMW seven series automobile with a temporary paper registration sticker ("SUBJECT PREMISES-2"), for evidence of violations of Title 18, United States Code, Section 1029(a)(5) (Access Device Fraud), Section 1344 (Bank Fraud) and Section 1028A (Aggravated Identify Theft). I have seen HUDSON drive SUBJECT PREMISES-2 and I have seen SUBJECT PREMISES-2 parked in the driveway of SUBJECT PREMISES-1. Because I do not know the vehicle identification number or registration number of SUBJECT PREMISES-2, this application for authority to search SUBJECT PREMISES-2 is conditioned on the vehicle being parked in the driveway of SUBJECT PREMISES-1 when I execute the search warrant at SUBJECT PREMISES-1.

### III..

#### PREMISES TO BE SEARCHED

9. This application seeks authorization to search the following location and vehicle (collectively, the "SUBJECT PREMISES"):

a. "SUBJECT PREMISES-1" -- The premises located at 205 West Fairview Boulevard, Inglewood, California 90302. SUBJECT PREMISES-1 is a one-story single family dwelling that is tan in color with white trim. The roof is light grey in color. The numbers "205"



are affixed with black lettering on the front of the residence. SUBJECT PREMISES-1 is located on the north side of West Fairview Boulevard. HUDSON lives at SUBJECT PREMISES-1.

b. "SUBJECT PREMISES-2" -- A dark grey color BMW seven series automobile with a temporary paper registration sticker. This application for authority to search SUBJECT PREMISES-2 is conditioned on the vehicle being parked in the driveway of SUBJECT PREMISES-1 when I execute the search warrant at SUBJECT PREMISES-1.

#### IV.

##### ITEMS TO BE SEIZED

10. Based on my training and experience, and the facts set forth below, I believe that there is probable cause to believe that the SUBJECT PREMISES contain and will contain evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1029 (Access Device Fraud), Section 1344 (Bank Fraud) and Section 1028A (Aggravated Identify Theft), and are particularly described as follows:

a. Letters, cards, envelopes, or other documents and mail matter, opened or unopened, addressed to an address other than SUBJECT PREMISES-1;

b. Letters, cards, envelopes, or other documents and mail matter, opened or unopened, addressed to SUBJECT PREMISES-1 and sent from financial institutions, credit card companies, public

storage facilities, any state's department of motor vehicles, or any governmental agencies;

c. United States currency if the total amount found exceeds \$1,000;

d. Indicia of occupancy, residency, ownership, or dominion and control of SUBJECT PREMISES-1 and SUBJECT PREMISES-2, such as leases, utility bills, canceled mail, credit card statements, bank account statements, checks, deposit slips, and check books;

e. Documents or materials containing personal information, such as social security numbers, dates of birth, names, addresses, bank account numbers, driver's license numbers, or credit card numbers;

f. Identification cards and/or driver's licenses, and materials, including plastic cards, cardstock, and laminates, that could be used in the fashioning of any false identification documents or access devices or counterfeit or unauthorized access devices, within the definition of 18 U.S.C. § 1029(e);

g. Birth certificates, death certificates, driver's licenses, credit cards, social security cards, passports, bank statements, credit card statements, credit card applications, credit reports, money orders, loan documents, leases, business cards, invoices, receipts, or any other identification document within the definition of 18 U.S.C. § 1028(d), bearing any name other than STANLEY

ALEXANDER HUDSON;

h. Documents reflecting electronic or telephone communications or transactions with bank, phone, or credit card companies, or with credit reporting agencies, as well as documents and materials reflecting credit card transactions with online businesses or websites;

i. Any credit card device and/or check-making equipment including, but not limited to, readers, encoders, printers, embossers, plastic cards, check card stock, and other related materials;

j. Any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature that either individually or in combination with another feature is used by an issuing authority on any identification document within the definition of 18 U.S.C. § 1028(d), or means of identification within the definition of 18 U.S.C. § 1028(d), to determine if the document is counterfeit, altered or otherwise falsified;

k. Any implement, impression, template, or electronic device that is specifically configured or primarily used for making an identification document within the definition of 18 U.S.C. § 1028(d), or a false identification document within the definition of 18 U.S.C. § 1028(d); and

l. Documents relating to the rental of any storage

facilities.

11. As used above, the terms records, documents, programs, applications or materials include records, documents, programs, applications or materials created, modified or stored in any form, including in digital form on any digital device. The term "digital device" includes any electronic device capable of storing and/or processing data in digital form, including: central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media; and security devices.

12. In searching for data capable of being read, stored or interpreted by a digital device, law enforcement personnel executing this search warrant will employ the following procedure:

a. Upon securing the premises, the law enforcement personnel executing the search warrant will, to the extent possible without requiring the use of special training in searching and seizing digital data, seek to determine if any digital device contains data falling within the scope of the items to be seized in the warrant. If they can make this determination without

jeopardizing the integrity of the digital data and a digital device contains data falling within the scope of the items to be seized in the warrant, that digital device will be seized. If they cannot make this determination, or they believe they cannot make this determination, without jeopardizing the integrity of the digital data, law enforcement personnel trained in searching and seizing digital data (the "computer personnel") will be consulted (either on-site or off-site) to determine whether the digital device can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data contained on the digital device.

b. If the digital device can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, it will be searched on-site and seized only if the search reveals it to be an item to be seized or to contain any data that falls within the list of items to be seized set forth herein.

c. If the digital device cannot be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, then the digital device will be seized and transported to an appropriate law enforcement laboratory for review. The digital device will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

d. In searching the digital device, the computer personnel may examine all of the data contained in the digital device to view their precise contents and determine whether the digital device and/or data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data fall within the list of items to be seized as set forth herein.

e. If the computer personnel seize the digital device pursuant to subparagraph (c) above, the computer personnel will initially search the digital device within a reasonable amount of time not to exceed 60 days from the date of execution of the warrant. If, after conducting such an initial search, the case agents determine that a digital device is an item to be seized or contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the digital device for further analysis; otherwise, the government will return the digital device. If the government needs additional time to determine whether the digital device is an item to be seized or contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original sixty day period from the date of execution of the warrant.

13. In order to search for data that are capable of being read or interpreted by a digital device, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above:

- a. Any digital device capable of being used to commit, further or store evidence of the offense listed above;
- b. Any equipment used to facilitate the transmission, creation, display, encoding or storage of digital data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices and optical scanners;
- c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, cellular telephones and personal digital assistants;
- d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software used in the digital device;
- e. Any applications, utility programs, compilers, interpreters and other software used to facilitate direct or indirect communication with the digital device;
- f. Any physical keys, encryption devices, dongles and

similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or data stored on the digital device.

V.

STATEMENT OF PROBABLE CAUSE

A. Summary of the Investigation

14. In or about February 2007, I initiated an investigation into a credit card fraud scheme operating in the Los Angeles area. The schemers were generally using fictitious names combined with true social security numbers to open fraudulent credit card accounts and having the credit cards sent to Commercial Mailings Receiving Agencies ("CMRAs"), commonly known as post office box addresses. The schemers were using multiple fraudulent identities, including variations of several identities.

15. My investigation resulted in an individual being arrested and charged in June 2008 with Bank Fraud, in violation of Title 18, United States Code, Section 1344. The indictment in that case alleges that, from February 2003 through December 2007, the charged defendant opened or caused to be opened over 30 fraudulent credit cards, causing financial institutions to suffer over \$500,000 in losses.



16. Based on information provided by a cooperating defendant and further investigation to date, I have discovered an additional 18 fraudulent credit cards that have caused financial institutions to suffer over \$250,000 in losses. These 18 fraudulent credit card accounts appear to be linked to the same fraudulent scheme alleged in the aforementioned indictment. The cooperating defendant has stated that HUDSON was directing the credit card fraud scheme.

17. My investigation has revealed that, by using multiple aliases, HUDSON was named as an authorized user on many of the 30 fraudulent credit cards identified in the initial phase of the investigation through June 2008. Further investigation has revealed that HUDSON, again using multiple aliases, is also named as an authorized user on many of the 18 recently-identified fraudulent credit cards. The 18 accounts were opened by using several of the same CMRA addresses that were used to open the approximately 30 accounts identified in the initial investigation. One of the CMRA addresses was opened with a fraudulent driver's license that had a picture of HUDSON on it.

18. As set forth in further detail below, my continuing investigation into HUDSON has also revealed that his residential trash recently contained a postal money order receipt. The receipt was for the purchase of two money orders totaling \$960. I traced the purchase of the two money orders to a bank debit card, the account

for which was opened with a minor's social security number that does not match the name on the bank account. I also traced the deposit of the two money orders and learned that one was deposited into a bank account that was also opened with a minor's social security number that does not match the name on that bank account.

19. My investigation into HUDSON also reveals that he maintains two fraudulent credit cards, opened with social security numbers of two deceased individuals, with a CMRA address opened in HUDSON's name. Finally, HUDSON has called a confidential source from a phone registered in the name "Brando Courtney" or "Brandon Courtney." In the course of my initial investigation, I identified five fraudulent credit card accounts opened in the name "Brandon Courtney" that have resulted in banks losing over \$162,000.

**B. Initiation of Credit Card Fraud Investigation in February 2007**

20. In or about February 2007, I was informed by J.P. Morgan Chase Bank ("Chase") Investigator Dawn Mercer ("Mercer") of a credit card fraud scheme operating in the Los Angeles area. Mercer informed me that she linked 26 fraudulent accounts through her analysis of balance transfers, addresses and telephone numbers identified via the Automated Number Identification system, which records the incoming telephone number of an account holder who calls the bank's customer service number. Mercer informed me that unknown suspects were perpetrating a "synthetic identity fraud" scheme in which the

fraudulently issued cards were shipped to various locations in Los Angeles County. Synthetic identity fraud is defined as receipt of credit by use of a fictitious name and a true social security number ("SSN"), which is in fact issued to a person other than the person applying for and receiving credit. Once credit is issued using the combination of real and fictitious identifying information, a new identity is established. Several of the 26 fraudulent accounts were opened over the Internet.

21. Mercer sent me the account profile and documents for the linked accounts involved in the aforementioned scheme. I reviewed the documentation provided by Mercer and by CMRAs that were identified by Chase. I noticed that several accounts used the same account addresses. I also concluded that one apparent part of the scheme was to add as an authorized user one or more individuals who are suspected to have been perpetrating the credit card fraud scheme. The apparent *modus operandi* of the schemers was to use fictitious identities to open the credit card accounts and then add themselves as authorized users. This way, the fraudulent accounts were not in the names of the schemers, allowing the schemers to be one level removed from the fraudulent activity. My investigation of the fraudulent credit card scheme, and analysis of CMRA applications and surveillance video, revealed several unknown suspects who were involved in this scheme.

22. I identified one of the suspects, however, during the course of my investigation. In or about June of 2008, I arrested the identified suspect pursuant to a federal arrest warrant for violations of Title 18, United States Code, Section 1344 (Bank Fraud) for the individual's role in the above described fraud scheme. The identified individual is charged in an indictment with several violations of 18 U.S.C. § 1344 for causing, from February 2003 through December 2007, financially insured financial institutions to issue over 30 fraudulent credit cards, resulting in over \$500,000 in losses to the financial institutions.

C. A Cooperating Defendant Identified HUDSON as Directing a Credit Card Fraud Scheme

23. In or about August of 2008, Secret Service Special Agent ("SSSA") James Spence and I interviewed a cooperating defendant (hereinafter, the "CD") regarding other individuals involved in his/her credit card fraud scheme. The CD provided us with the following information:

a. The CD worked with an individual named "Stanley Alexander" (later identified to be HUDSON), who the CD described as:

- i. A black male;
- ii. Approximately six feet tall;
- iii. Weighing approximately 270 pounds; and
- iv. Approximately 40 years old.

b. HUDSON drives a brand new BMW seven series, black or dark grey in color, and resides in the city of Inglewood near the intersection of La Tijera and S. La Cienega.

c. HUDSON would give the CD names and addresses and instruct him to obtain fake identifications with that information. The CD would obtain fake identifications for himself/herself in the names provided by HUDSON. The CD would then open mail boxes at various CMRA's throughout the Los Angeles County area with the fake identifications that the CD obtained by using information that HUDSON provided to him/her.

d. HUDSON paid the CD to drive to the various CMRA's, pick up mail, and deliver the mail to HUDSON. HUDSON paid the CD to do this for approximately seven years.

e. HUDSON also paid the CD to do the following:

i. Purchase gift cards from various stores with the credit cards that were sent to the various CMRA locations in Los Angeles County;

ii. Deposit checks for HUDSON into bank accounts set up by HUDSON; and

iii. Go to Automated Teller Machines ("ATMs") to withdraw money.

f. The CD went with HUDSON to two storage units located in the Los Angeles County area. On another occasion, the CD also

went to renew the storage unit for HUDSON. The CD believes HUDSON keeps fraudulent documents in one or more storage units.

24. Based upon my training and experience, and information related to me by other experienced law enforcement personnel who specialize in the investigation of financial and identity theft crimes, I have learned that it is common practice for criminal groups and individuals to use storage units as a place to hold, maintain, hide, conceal, and store stolen checks, credit cards, documents and other materials relating to their criminal activities. By hiding the tools and fruits of credit card fraud and identity theft in storage units, they attempt to avoid being identified and arrested. In addition, I have learned that criminal groups and individuals often use storage units to conceal fraud contraband. The storage units may also be used to hide keys, contracts and rental agreements for other places concealing contraband.

D. Identification of HUDSON and HUDSON's Connection to the Bank Fraud Charges Against the CD

25. In or about August of 2008, SSSA Spence and I drove around the residential areas near the intersection of La Tijera and S. La Cienega in the city of Inglewood. We noticed a dark grey color BMW seven series (SUBJECT PREMISES-2), which matched the description provided by the CD, driving in the residential area and decided to follow the vehicle. We observed the vehicle pull into the driveway

at 205 West Fairview Boulevard, Inglewood, California 90302 (SUBJECT PREMISES-1). SUBJECT PREMISES-1 is located in the vicinity of the La Tijera and S. La Cienega intersection, as the CD had stated. I observed a black male closely fitting the description given by the CD exit the vehicle and walk into SUBJECT PREMISES-1. The dark grey color BMW seven series vehicle had a paper registration sticker. Because I did not want to compromise my investigation, I did not attempt to get close to SUBJECT PREMISES-2, which was parked in the back of the driveway of SUBJECT PREMISES-1, to identify the vehicle's registration number.

26. In or about August 2008, I searched in law enforcement databases and learned that the owner of SUBJECT PREMISES-1 is STANLEY ALEXANDER HUDSON, born on XX/XX/1961. Furthermore, I searched California Department of Motor Vehicles ("DMV") databases and learned that California Driver's License ("CDL") NXXX5805 is assigned to STANLEY ALEXANDER HUDSON. I subsequently retrieved a color California DMV photograph of HUDSON and retained this for future reference.

27. DMV records indicate that HUDSON resides at 10736 Jefferson Boulevard # 263, Culver City, CA 90245, which is a CMRA address. On October 24, 2008, however, a postal representative confirmed that HUDSON receives mail at SUBJECT PREMISES-1. Further, my search of law enforcement databases reveals that a female with

the last name "Hudson" has a utility registered in her name at SUBJECT PREMISES-1. The bills for the utility are sent to the same CMRA address that appears on HUDSON's CDL.

28. I searched law enforcement databases to determine whether HUDSON is the registered owner of SUBJECT PREMISES-2. I did not find HUDSON listed as the registered owner of SUBJECT PREMISES-2, or as the current registered owner of any other vehicle. I have not been able to ascertain the registered owner of SUBJECT PREMISES-2 because I do not know the vehicle's registration number.

29. I compared HUDSON's driver's license picture to surveillance video footage and CMRA applications that I had obtained during my initial investigation of the CD and learned the following:

a. I compared the color photo on HUDSON'S driver's license to video surveillance that I had previously obtained from Circuit City and concluded that HUDSON appeared to be the same person on the video who purchased electronics at a Circuit City store in Los Angeles, California, in or about February of 2008. HUDSON purchased those electronics by using gift cards worth approximately \$300 that the CD had obtained in or about February 2008. The CD had purchased gift cards worth \$600 by charging them to one of the 30 fraudulent credit cards identified in the initial phase of my investigation.

b. During the investigation of the CD, I obtained



numerous applications to open mail boxes at CMRA's in the Los Angeles County area. The mail boxes had been opened with fraudulent driver's licenses, including CMRA box number 375 at the Village Mail Box located at 3175 S. Hoover St., Los Angeles, California ("HOOVER CMRA"), which was opened in the name of Josh Webber. Fraudulent driver's license number BXXX3461, in the name of Josh V. Webber, was used to open box 375 at the HOOVER CMRA. I compared the photograph of HUDSON from his legitimately issued CDL NXXX5805 to the picture on the recovered fraudulent CDL BXXX3461 (provided to open the HOOVER CMRA) and concluded that the picture on the fraudulent CDL appears to match the picture of HUDSON. The HOOVER CMRA address was utilized to open a fraudulent credit card account on which both the CD and HUDSON were added as authorized users.

30. In or about August of 2008, I reviewed the credit card accounts identified in my previous investigation of the CD and noted that a variation of HUDSON's name was added to many of those accounts as an authorized user. I sent out notifications to various banks, including Chase and Discover, alerting them of a new suspect involved in the synthetic identity fraud scheme. I instructed them to check for any additional accounts to which HUDSON was added as an authorized user. Chase and Discover informed me that they identified over 18 accounts on which variations of HUDSON's name were added as an authorized user, including one account opened with the HOOVER CMRA

address. They also informed me that most of the accounts have been charged off or flagged as fraud. Several of the 18 fraudulent accounts were opened over the Internet.

31. In or about August 2008, I reviewed documentation provided by Chase and Discover for the newly-identified fraudulent accounts and determined that several of the fraudulent accounts used the same account addresses as those identified in my initial investigation of the CD, including the HOOVER CMRA address. I provided the account holder names and corresponding Social Security Number ("SSN") for each of the linked fraudulent accounts identified by Chase and Discover to Social Security Administration ("SSA") Special Agent ("SA") Paul Yokoyama. SSA SA Yokoyama informed me that the following account holder names did not correspond with their purported SSNs, which were used to open the identified Chase and Discover credit card accounts:

///

///

///

NAME	SSN
Rodney Z. Hudson	XXX-XX -0019
Stanley K. Ross	XXX-XX -2765
Nicholas P. Duncan	XXX-XX -8332
Nicholas K. Hudson	XXX-XX -7650
Jonathan Houston	XXX-XX -1861
Richard F. Ross	XXX-XX -9532
Thomas V. Anderson	XXX-XX -9742
Jonathan P. Webber	XXX-XX -0011
Nicholas K. Jenkins	XXX-XX -4487
Raymond D. Ross	XXX-XX -6432
Kenneth Z. Anderson	XXX-XX -3904
Stanley T. Letterman	XXX-XX -0132
Patrick V. Anderson	XXX-XX -1963
Rodney F. Alexander,	XXX-XX -7632
Luther F. Johnson	XXX-XX -1129
Stanley L. Moore	XXX-XX -1109

32. After reviewing the account reports from Chase and Discover, I determined that the combined loss sustained by the aforementioned financial institutions for the 18 newly-identified fraudulent accounts linked to HUDSON is approximately \$252,775.66. This loss is in addition to losses of over \$500,000 on the accounts previously identified during my initial investigation through June 2008.

33. Further, as discussed below, HUDSON has made phone calls from a phone under the name "Brando Courtney" or "Brandon Courtney." During my initial investigation, I identified five fraudulent credit card accounts opened in the name "Brandon Courtney" that resulted

in losses of over \$162,000.

**E. Investigation at the SUBJECT PREMISES**

34. On or about September 3, 2008, at approximately 5 a.m., Postal Inspector Noah Thompson and I picked up trash left outside SUBJECT PREMISES-1. At that time, I noticed that the same dark grey color BMW seven series that I had seen HUDSON driving in August 2008, was parked in the back of the driveway of SUBJECT PREMISES-1.

35. Later on September 3, 2008, Inspector Thompson and I examined a bag of trash that we picked up from outside SUBJECT PREMISES-1. Inside the trash, we found a receipt for purchases of postal money orders on August 22, 2008, from the Crenshaw Post Office in Los Angeles, California. Inside the trash, we also found mail addressed to the same woman with the last name "Hudson," in whose name a utility is registered at SUBJECT PREMISES-1.

36. In or about September 2008, I searched Postal Service databases for the aforementioned receipt found in the trash of SUBJECT PREMISES-1 and learned the following:

a. Two postal money orders were purchased, one for \$160.00 and one for \$800.00, in the transaction depicted in the recovered receipt; and

b. Debit card number XXXX-XXXX-XXXX-8500 was used to pay for the money orders.

**F. Investigation of the Debit Card Used to Purchase the Postal Money Orders Connected to HUDSON**

37. I searched in law enforcement databases and learned that debit card number XXXX-XXXX-XXXX-8500 is a Bank of America debit card. In or about September of 2008, I contacted Bank of America Investigator Peggy Thompson regarding the aforementioned debit card and she informed me of the following:

a. Debit card number XXXX-XXXX-XXXX-8500 is associated with checking account XXX-X36-85, which was opened in the name of "Raymond V. Courtney."

b. SSN XXX-XX-9971 was used to open the aforementioned account.

38. In or about September 15, 2008, I contacted SSA SA Yokoyama regarding SSN XXX-XX-9971. SSA SA Yokoyama stated SSN XXX-XX-9971 is not associated with the name "Raymond V. Courtney." SSA SA Yokoyama also informed me that SSN XXX-XX-9971 belongs to a minor.

**G. Investigation of the Deposit of the Postal Money Orders Connected to HUDSON**

39. In or about September 2008, I retrieved images of the two postal money orders identified in the receipt I found in the trash of SUBJECT PREMISES-1 and learned the following:

a. Postal money order number XXXXXX3697, in the amount of \$800.00, was deposited into a Bank of America account in or about August 25, 2008.

b. Postal money order number XXXXXX3686, in the amount of \$160.00, was deposited into a Wells Fargo Bank account in or about August 28, 2008.

40. On or about September 8, 2008, I contacted Bank of America and Wells Fargo Bank and they informed me of the following:

Bank of America

a. Bank of America Investigator Pauline Villescas informed me that postal money order number XXXXXX3697 was deposited into Bank of America account number XX-XX-XXXXX-X1048 on August 25, 2008, at a Bank of America in the Los Angeles County area. The account was opened in the name of M.R., and SSN XXX-XX-3264 was used to open the account. Villescas also informed me that the account was opened in the state of Arizona with Arizona driver's license number DXXXX8900 in the name of M.R.

Wells Fargo Bank

b. Wells Fargo Bank Investigator Lauryen Kato informed me that postal money order number XXXXXX3686 was deposited into Wells Fargo bank account number XXXXXX3140 on August 28, 2008, at a Wells Fargo Bank branch in the Los Angeles County area. The account was opened online in the name of M.R., and SSN XXX-XX-8960 was used to open the account.

41. In or about September 2008, I contacted SSA SA Yokoyama regarding SSN XXX-XX-3264 and SSN XXX-XX-8960. SSA SA Yokoyama

informed me that SSN XXX-XX-3264 is a valid SSN and does belong to a person by the name of M.R., but SSN XXX-XX-8960 is not associated with the name M.R. He also informed me that SSN XXX-XX-8960 belongs to a minor.

42. On or about September 17, 2008, I contacted Arizona Postal Inspector Gary Nork regarding Arizona driver's license DXXXX8900. Inspector Nork informed me he searched Arizona DMV databases and learned that it is a valid driver's license in the name of M.G.F.R. Inspector Nork subsequently sent me a copy of the driver's license photo. I reviewed the copy of driver's license DXXXX8900 in the name of M.G.F.R. and observed that the individual is a white male.

**H. HUDSON Has No Known Employment History**

43. On or about September 15, 2008, I sent HUDSON'S name and identifying information to Employment Development Division ("EDD"), which keeps records of an individual's employment history for approximately the preceding 18 months. On or about the same date, I received a response from EDD stating that it found no reported employment for HUDSON in its databases.

**I. HUDSON Has Opened Two Bank of America Credit Cards Using a CMRA Address and Social Security Numbers of Dead People**

44. In or about September of 2008, Discover Bank Investigator Maria Micioni ("Micioni") provided me with bank documents of additional accounts related to my synthetic identity fraud

investigation. After reviewing the bank documents and speaking with Micioni, I learned the following:

a. Discover Bank credit card account

XXXX-XXXX-XXXX-2699 was opened in or about October 2002 in the name of "Stanley Alexander." "Stanley Alexander" gave SSN XXX-XX-1712 and date of birth ("DOB") XX/XX/1961, on the application. The mailing address listed on the aforementioned account is 10321 National Blvd., #20, Los Angeles, California 90034.

b. Discover Bank credit card account

XXXX-XXXX-XXXX-3930 was opened in or about July of 1994 in the name of "Robert L. Folks," with an added authorized user of "Stanley A. Hudson." "Robert L. Folks" used SSN XXX-XX-3017 and DOB XX/XX/1961, on the application. The 1961 DOB used to open credit card account XXXX-XXXX-XXXX-2699 is different from the 1961 DOB used to open credit card account XXXX-XXXX-XXXX-3930. The mailing address listed on account XXXX-XXXX-XXXX-3930, however, is also 10321 National Blvd., #20, Los Angeles, California 90034.

45. In or about September of 2008, I went to 10321 National Blvd., #20, Los Angeles, California 90034 and learned that National Blvd. Self Storage and CMRA ("National CMRA") is located there. After reviewing the application for Box number 20, I learned the following:

a. Box number 20 was opened in 1999 in the name of



"Stanley Alexander."

b. CDL NXXX5805, in the name of "Stanley Alexander," was provided to open box number 20. As noted above, CDL NXXX5805 is currently in the name of STANLEY ALEXANDER HUDSON.

46. While I was at National CMRA, I spoke to an employee who confirmed that an individual fitting the description of HUDSON has been coming to pick up mail delivered to Box number 20 for several years.

47. In or about September 2008, I compared the copy of the CDL provided to open Box number 20 to HUDSON'S current CDL and determined the following:

- a. CDL number NXXX5805 is HUDSON's current CDL number;
- b. The DOB listed on the two CDLs is the same;
- c. The expiration date on the CDL provided to open Box number 20 was August 20, 2000; and
- d. The photo on the CDL that expired on August 20, 2000, appears to be a younger picture of HUDSON.

48. In or about September 2008, I received surveillance video from the National CMRA for September 18, 2008. I watched the surveillance video and learned the following:

- a. The video depicts an individual who appears to be HUDSON driving up to the National CMRA in a dark grey color BMW seven series (the BMW seven series appears to be the same one that I observed

at SUBJECT PREMISES-1 during my investigation of HUDSON);

b. HUDSON walked into the National CMRA and an employee of National CMRA handed HUDSON various pieces of mail matter from box number 20; and

c. HUDSON exited National CMRA and drove away in the aforementioned BMW.

49. On or about September 20, 2008, I contacted SSA SA Yokoyama regarding SSN XXX-XX-1712, used with the name "Stanley Alexander" to open Discover Bank credit card XXXX-XXXX-XXXX-2699, and regarding SSN XXX-XX-3017, used with the name "Robert L. Folks" to open Discover Bank credit card XXXX-XXXX-XXXX-3930. On or about September 23, 2008, SSA SA Yokoyama informed me that SSN XXX-XX-1712 is a valid SSN but does not belong to a person by the name of "Stanley Alexander." SSN XXX-XX-1712 belongs to a person who died in 1965. SSN XXX-XX-3017 did belong to "Robert L. Folks," but Folks died in 1989.

J. HUDSON Has Been Calling a Confidential Source from a Phone Number Registered in a Name Connected to Fraudulent Credit Card Accounts

50. In October 2008, I spoke to a confidential source ("CS") regarding telephone calls that he/she had received from an individual who he/she knows as "Stanley Alexander" (HUDSON). The CS informed me that he/she received calls from "Stanley Alexander" from a phone that the CS's caller identification showed as registered to either "Brando Courtney" or "Brandon Courtney." The CS recognized the

voice of the person calling from the phone registered to "Brando Courtney" or "Brandon Courtney" as "Stanley Alexander" (HUDSON).

**K. The Initial Investigation of the CD Identified Five Fraudulent Credit Cards Opened Under the Name "Brandon Courtney" that Resulted in Losses Exceeding \$162,000**

51. In October 2008, I reviewed the loss analysis provided by banks during my initial investigation of the CD. That analysis identified five fraudulent credit cards opened in the name "Brandon Courtney." The combined loss on these five fraudulent credit cards was approximately \$162,450.

**L. HUDSON Lives at or Controls SUBJECT PREMISES-1**

52. The following evidence, discussed above, establishes that HUDSON lives at or controls SUBJECT PREMISES-1:

- a. A postal representative stated on October 24, 2008, that HUDSON receives mail at SUBJECT PREMISES-1;
- b. HUDSON is the owner of SUBJECT PREMISES-1;
- c. In or about August 2008, I observed a male closely fitting the description of HUDSON park SUBJECT PREMISES-2 in the driveway of SUBJECT PREMISES-1 and enter SUBJECT PREMISES-1;
- d. At approximately 5:00 a.m. on September 3, 2008, I observed SUBJECT PREMISES-2 parked in the back of the driveway of SUBJECT PREMISES-1;
- e. The CD stated that HUDSON resides in the city of Inglewood near the intersection of La Tijera and S. La Cienega.

SUBJECT PREMISES-1 is in the city of Inglewood, in the vicinity of La Tijera and S. La Cienega;

f. A female with the last name "Hudson" has a utility registered in her name at SUBJECT PREMISES-1 and the bills for the utility account are sent to the same CMRA address that appears on HUDSON's CDL; and

g. When I searched the trash that I picked up from outside SUBJECT PREMISES-1, I found mail addressed to the same female who has a utility registered at SUBJECT PREMISES-1.

VI.

CONCLUSION

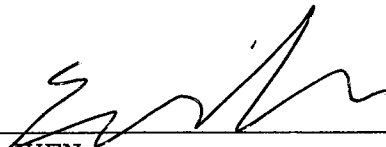
53. Based on the foregoing facts, I respectfully submit that there is probable cause to believe that SUBJECT PREMISES-1 and SUBJECT PREMISES-2 contain and will contain evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1029 (Access Device Fraud), Section 1344 (Bank Fraud) and Section 1028A (Aggravated Identify Theft).

///

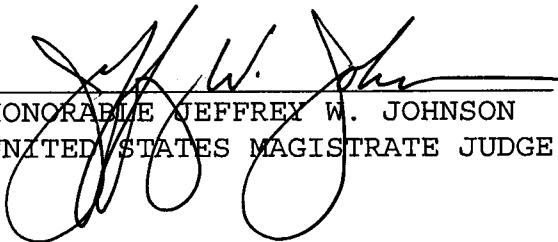
///

///

54. Based on the foregoing facts, I also submit that there is probable cause to believe that STANLEY ALEXANDER HUDSON has violated Title 18, United States Code, Section 1029(a)(5) (Access Device Fraud).

  
\_\_\_\_\_  
ERIC SHEN  
United States Postal Inspector

Subscribed and sworn to before me  
this 28<sup>th</sup> day of October, 2008

  
\_\_\_\_\_  
HONORABLE JEFFREY W. JOHNSON  
UNITED STATES MAGISTRATE JUDGE